



THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

Counting factorisations of monomials over rings of integers modulo N

Citation for published version:

Wright, J & Hickman, J 2019, 'Counting factorisations of monomials over rings of integers modulo N ', *Journal de Théorie des Nombres*, vol. 31, 1, pp. 255-282. <https://doi.org/10.5802/jtnb.1079>

Digital Object Identifier (DOI):

[10.5802/jtnb.1079](https://doi.org/10.5802/jtnb.1079)

Link:

[Link to publication record in Edinburgh Research Explorer](#)

Document Version:

Peer reviewed version

Published In:

Journal de Théorie des Nombres

General rights

Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.



Counting factorisations of monomials over rings of integers modulo N

par JONATHAN HICKMAN et JAMES WRIGHT

RÉSUMÉ. Une borne supérieure optimale est obtenue pour le nombre de façons d’exprimer le monôme X^n en tant que produit de facteurs linéaires sur $\mathbb{Z}/p^\alpha\mathbb{Z}$. La démonstration utilise la récurrence pour estimer le nombre de solutions d’un certain système de congruences polynômiaux. La méthode s’applique également à des systèmes de congruences polynomiaux plus généraux qui satisfont une hypothèse de non dégénérescence.

ABSTRACT. A sharp bound is obtained for the number of ways to express the monomial X^n as a product of linear factors over $\mathbb{Z}/p^\alpha\mathbb{Z}$. The proof relies on an induction-on-scale procedure which is used to estimate the number of solutions to a certain system of polynomial congruences. The method also applies to more general systems of polynomial congruences that satisfy a *non-degeneracy* hypothesis.

1. Introduction

Let $\alpha, n \in \mathbb{N}$ and $p \in \mathbb{N}$ be prime. One purpose of this note is to provide a precise count for the number of factorisations of the monomial X^n into linear factors over $\mathbb{Z}/p^\alpha\mathbb{Z}$. That is, (after normalising) one wishes to determine the value of

$$\mathbf{N}(\vec{0}_n; p^\alpha) := p^{-\alpha n} \# \left\{ (x_1, \dots, x_n) \in [\mathbb{Z}/p^\alpha\mathbb{Z}]^n : X^n \equiv \prod_{j=1}^n (X - x_j) \pmod{p^\alpha} \right\}.$$

If $\alpha = 1$, then $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field and the polynomial ring $\mathbb{F}_p[X]$ is a unique factorisation domain and so there is only one possible factorisation

2000 *Mathematics Subject Classification.* 11A07, 11A51.

Mots-clefs. Factorising polynomials, congruence equations, Igusa conjecture.

The authors would like to thank Julia Brandes and Jordan Ellenberg for interesting discussions on topics related to this project. They also wish to thank Douglas Howroyd for assisting with the preparation of the manuscript for publication. This material is based upon work supported by the National Science Foundation under Grant No. DMS-1440140 while the first author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2017 semester.

of X^n . In general, however, there are many different factorisations: for example,

$$X^2 \equiv (X - 3)(X - 6) \pmod{9}.$$

Unfortunately, the general statement of the results is slightly involved. Things become much cleaner, however, if n is assumed to be a triangular number, and it is instructive to first consider this case. In particular, letting $\Delta_r := \frac{r(r+1)}{2}$ denote the r th triangular number, the following estimate holds.

Proposition 1.1. *If $n = \Delta_r$ for some $r \in \mathbb{N}$ with $r \geq 2$ and p is a sufficiently large prime, then¹*

$$\mathbf{N}(\vec{0}_n; p^\alpha) \ll_n \alpha p^{-\alpha r}$$

holds for all $\alpha \in \mathbb{N}$. The result is sharp for all $n \neq 3$ in the sense that the reverse inequality also holds for infinitely many α .

When n is not a triangular number, the asymptotics of $\mathbf{N}(\vec{0}_n; p^\alpha)$ are not readily expressed in a single compact formula. In fact, for $n = 2$ it is a simple matter to see that $\mathbf{N}(\vec{0}_2; p^\alpha) = p^{-3\alpha/2}$ when α is even and $\mathbf{N}(\vec{0}_2; p^\alpha) = p^{-(3\alpha+1)/2}$ when α is odd.

In order to state the general form of Proposition 1.1, first define

$$e_n(\alpha, r) := r\alpha + (n - \Delta_r) \cdot \begin{cases} \lceil \frac{\alpha}{r+1} \rceil & \text{if } \Delta_r \leq n \\ \lceil \frac{\alpha}{r} \rceil - 1 & \text{if } \Delta_r \geq n \end{cases}$$

for $0 \leq r \leq n-1$. Let $e_n(\alpha) := \min\{e_n(\alpha, r) : r \in R_n(\alpha)\}$ where

$$R_n(\alpha) := \{0\} \cup \{1 \leq r \leq n-1 : \lceil \frac{\alpha}{r+1} \rceil < \lceil \frac{\alpha}{r} \rceil\}.$$

and let

$$[\alpha]^{\delta_n(\Delta)} := \begin{cases} \alpha & \text{if } n = \Delta_r \text{ for some } r \geq 1 \text{ and } r \in R_n(\alpha) \\ 1 & \text{otherwise} \end{cases}.$$

The main theorem is as follows.

Theorem 1.2. *If $n \in \mathbb{N}$, $n \neq 3$ and p is a sufficiently large prime, then*

$$(1.1) \quad \mathbf{N}(\vec{0}_n; p^\alpha) \sim_n [\alpha]^{\delta_n(\Delta)} p^{-e_n(\alpha)}$$

holds for all $\alpha \in \mathbb{N}$.

Explicitly, the proof shows that the upper bound in (1.1) holds if $p > n$. Curiously, the $n = 3$ case behaves differently and, in particular, the asymptotics for $\mathbf{N}(\vec{0}_3; p^\alpha)$ depend on the congruence class of p modulo 3: see Lemma 5.1, below.

¹Given a (possibly empty) list of objects L , for real numbers $A, B \geq 0$ the notation $A \ll_L B$ or $B \gg_L A$ signifies that $A \leq C_L B$ for some constant $C_L \geq 0$ depending only on the objects in the list. Furthermore, $A \sim_L B$ signifies that $A \ll_L B \ll_L A$.

The definition of the exponent $e_n(\alpha)$ is somewhat complicated and it is useful to consider some examples. For instance, when $n = 2$ it follows that $e_2(\alpha, 0) = 2\alpha$ and $e_2(\alpha, 1) = \alpha + \lceil \frac{\alpha}{2} \rceil$ for all $\alpha \in \mathbb{N}$, whilst $R_2(1) = \{0\}$ and $R_2(\alpha) = \{0, 1\}$ when $\alpha \geq 2$. Thus, one deduces that $e_2(\alpha) = e_2(\alpha, 1)$ and $[\alpha]^{\delta_2(\Delta)} = 1$ for all $\alpha \in \mathbb{N}$. Therefore, $[\alpha]^{\delta_2(\Delta)} p^{-e_2(\alpha)} = p^{-3\alpha/2}$ when α is even and $[\alpha]^{\delta_2(\Delta)} p^{-e_2(\alpha)} = p^{-(3\alpha+1)/2}$ when α is odd and so (1.1) yields

$$\mathbf{N}(\vec{0}_2; p^\alpha) \sim p^{-3\alpha/2} \quad \text{or} \quad p^{-(3\alpha+1)/2},$$

depending on whether α is even or odd, respectively. As noted earlier, these asymptotics are in fact an equality.

It is also instructive to understand how Theorem 1.2 relates to Proposition 1.1. First note that, by a simple computation,

$$\begin{aligned} e_n(\alpha, r-1) - e_n(\alpha, r) &\geq 0 \quad \text{for } \Delta_r \leq n, \\ e_n(\alpha, r+1) - e_n(\alpha, r) &\geq 1 \quad \text{for } \Delta_r \geq n \end{aligned}$$

and, consequently, $e_n(\alpha) \geq \min\{e_n(\alpha, r_n^-), e_n(\alpha, r_n^+)\}$ with equality if $r_n^-, r_n^+ \in R_n(\alpha)$ where

$$r_n^- := \max\{r \geq 0 : \Delta_r \leq n\} \quad \text{and} \quad r_n^+ := \min\{r \geq 0 : \Delta_r \geq n\}.$$

In general, either $e_n(\alpha, r_n^-)$ or $e_n(\alpha, r_n^+)$ can achieve the minimum: compare, for instance, the case $n = 5$, $\alpha = 3k$ with $n = 5$, $\alpha = 3k + 1$ for any $k \in \mathbb{N}$. However, if $n = \Delta_r$ is triangular, then $r_n^- = r_n^+ = r$ and so

$$e_n(\alpha) \geq e_n(\alpha, r) = r\alpha \quad \text{with equality if } r \in R_n(\alpha).$$

Note that the right-hand exponent is precisely that appearing in Proposition 1.1. It is easy to verify that

$$\begin{aligned} \{r \in \mathbb{N} : \lceil \frac{\alpha}{r+1} \rceil \neq \lceil \frac{\alpha}{r} \rceil\} &= \bigcup_{k \in \mathbb{N}} \{r \in \mathbb{N} : \lceil \frac{\alpha}{r+1} \rceil = \lceil \frac{\alpha}{r} \rceil = k\} \\ &= \bigcup_{k \in \mathbb{N}} \{r \in \mathbb{N} : \alpha \leq kr \leq \alpha + r - k\} \end{aligned}$$

and so if α is sufficiently large (in particular, if $\alpha > (n-1)^2$), then $R_n(\alpha) = \{0, 1, \dots, n-1\}$ and one has $e_n(\alpha) = \min\{e_n(\alpha, r_n^-), e_n(\alpha, r_n^+)\}$ with $e_n(\alpha) = \alpha r$ if $n = \Delta_r$. On the other hand, if $\alpha = 1$, then $R_n(1) = \{0\}$ for all $n \in \mathbb{N}$ and so $e_n(1) = e_n(1, 0) = n$, which is consistent with the unique factorisation property.

Observe that Theorem 1.2 can be recast as an estimation of the number of solutions to a certain system of congruence equations. In particular, by the classical Newton–Girard formulæ (see, for instance, [18, (2.11')]), if $p > n$, then $\mathbf{N}(\vec{0}_n; p^\alpha)$ is precisely the normalised number of solutions in $[\mathbb{Z}/p^\alpha\mathbb{Z}]^n$ to the system

$$P_k(X_1, \dots, X_n) \equiv 0 \pmod{p^\alpha} \quad \text{for } 1 \leq k \leq n$$

where P_k is the k th power sum, given by

$$P_k(X_1, \dots, X_n) := X_1^k + \dots + X_n^k.$$

At this point some contextual remarks are in order.

Remark 1.3.

- 1) Rather than restrict to monomials, given an n -tuple $\vec{y} = (y_1, \dots, y_n) \in [\mathbb{Z}/p^\alpha\mathbb{Z}]^n$, one could estimate the normalised count $\mathbf{N}(\vec{y}; p^\alpha)$ of the number of factorisations

$$\prod_{j=1}^n (X - y_j) \equiv \prod_{j=1}^n (X - x_j) \pmod{p^\alpha}.$$

For $p > n$, this is equivalent to counting solutions to the system

$$P_k(X_1, \dots, X_n) \equiv P_k(y_1, \dots, y_n) \pmod{p^\alpha} \quad \text{for } 1 \leq k \leq n.$$

If the components of \vec{y} are well-separated in the p -adic sense, then $\mathbf{N}(\vec{y}; p^\alpha)$ can be bounded (in fact, explicitly determined) via Hensel lifting, as observed in [11] (see also [20], which treats very general systems of congruences under much stronger ‘non-degeneracy’ hypotheses). Theorem 1.2 corresponds to the case $\vec{y} = \vec{0}_n$, which is a highly degenerate situation where there is no p -adic separation between the components of \vec{y} , and therefore acts as a counterpoint to the observations of [11].

- 2) The problem of counting factorisations of polynomials arose naturally in a recent study of the so-called *Fourier restriction phenomenon* for curves over $\mathbb{Z}/N\mathbb{Z}$ [11] (see also [5] and [10] for related questions). Fixing a polynomial curve $\gamma: \mathbb{Z}/N\mathbb{Z} \rightarrow [\mathbb{Z}/N\mathbb{Z}]^n$, the Fourier restriction problem involves the estimation of weighted exponential sums

$$(1.2) \quad \mathcal{E}G(\vec{y}) := \sum_{x \in \mathbb{Z}/N\mathbb{Z}} G(x) e^{2\pi i \gamma(x) \cdot \vec{y}/N}$$

defined for any coefficient function $G: \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$. In [11] a conjectural upper bound for $\mathbf{N}(\vec{y}; p^\alpha)$ is stated and a proof is given under additional hypotheses on \vec{y} (see item 1). Moreover, good control over $\mathbf{N}(\vec{y}; p^\alpha)$ is shown to imply favourable estimates for (1.2) in the prototypical case where $\gamma(x) := (x, x^2, \dots, x^n)$. The precise estimate of Theorem 1.2 does not appear to be directly applicable to Fourier restriction theory, but it is likely that the methods of proof will be useful in future studies. Furthermore, the problem of counting factorisations of monomials over $\mathbb{Z}/N\mathbb{Z}$ is arguably of some inherent interest.

- 3) Generalising the above notation, let $\mathbf{N}(\vec{0}_n; N)$ denote the normalised number of factorisations of X^n modulo N for $N \in \mathbb{N}$. By the Chinese

remainder theorem, $\mathbf{N}(\vec{0}_n; N)$ is a multiplicative function of N . If all the prime factors p of N satisfy $p > n$, then Theorem 1.2 implies that for all $\varepsilon > 0$ there exists a constant $C_{\varepsilon, n}$ such that

$$(1.3) \quad \mathbf{N}(\vec{0}_n; N) \leq C_{\varepsilon, n} N^\varepsilon \prod_{p|N} p^{-e_n(\text{ord}_p(N))}$$

where the product is over all prime factors of N and the integer $\text{ord}_p(N)$ is the multiplicity of the prime divisor p (so that $N = \prod_{p|N} p^{\text{ord}_p(N)}$). Indeed, Theorem 1.2 immediately yields (1.3) with $C_{\varepsilon, n} N^\varepsilon$ replaced with

$$C_n^{\omega(N)} \prod_{p|N} \text{ord}_p(N) \leq C_n^{\omega(N)} \left(\frac{\log N}{\omega(N)} \right)^{\omega(N)}$$

where $\omega(N) := \sum_{p|N} 1$ is the number of distinct prime divisors of N . Note that, as a simple and well-known consequence of Tchebychev's theorem on the size of the prime counting function,

$$\omega(N) \ll \frac{\log N}{\log \log N}.$$

By combining these observations, and considering the cases $\omega(N) \geq \varepsilon \cdot \log N / \log \log N$ and $\omega(N) < \varepsilon \cdot \log N / \log \log N$ separately, one readily deduces (1.3).

- 4) The authors have not attempted to optimise the values of the implied constants in Theorem 1.2 (that is, neither the size of the dimensional constant in (1.1), nor the lower bound on p). It is likely that improvements would follow from a more thorough analysis of systems of power sums over finite fields.

Theorem 1.2 is a consequence of a more general result concerning *non-degenerate* systems of congruences.²

Definition 1.4. An m -tuple of homogeneous polynomials $\vec{f} = (f_1, \dots, f_m) \in \mathbb{Z}[X_1, \dots, X_n]$ with $1 \leq m \leq n$ is said to be non-degenerate over \mathbb{F}_p for a prime p if for each $1 \leq r \leq m$ one has

$$\text{rank} \frac{\partial(f_1, \dots, f_r)}{\partial(X_1, \dots, X_n)}(x) = r$$

whenever $x \in \mathbb{P}^{n-1}(\overline{\mathbb{F}}_p)$ satisfies $f_k(x) = 0$ for all $1 \leq k \leq r$.

Here $\overline{\mathbb{F}}_p$ denotes the algebraic closure of the p -field \mathbb{F}_p and $\mathbb{P}^{n-1}(\overline{\mathbb{F}}_p)$ the $(n-1)$ -dimensional projective space over $\overline{\mathbb{F}}_p$. Any $f \in \mathbb{Z}[X_1, \dots, X_n]$ can be

²The notion of non-degeneracy discussed here is distinct from that appearing above in Remark 1.3 1).

considered a polynomial over \mathbb{F}_p by reducing the coefficients modulo p ; if f is homogeneous, then it can also be considered a polynomial over $\mathbb{P}^{n-1}(\overline{\mathbb{F}}_p)$.

For $1 \leq m \leq n$ let $\vec{f} = (f_1, \dots, f_m) \in \mathbb{Z}[X_1, \dots, X_n]^m$ be an m -tuple of polynomial mappings, where each f_k is homogeneous of degree d_k and $1 \leq d_1 \leq \dots \leq d_m$ and suppose that \vec{f} is non-degenerate over \mathbb{F}_p for some prime p . For $\alpha \in \mathbb{N}$ one wishes to estimate

$$\mathcal{N}(\vec{f}; p^\alpha) := p^{-\alpha n} \# \left\{ \vec{x} \in [\mathbb{Z}/p^\alpha \mathbb{Z}]^n : f_k(\vec{x}) \equiv 0 \pmod{p^\alpha} \text{ for } 1 \leq k \leq m \right\}.$$

In order to state the results, let $\sigma_r := \sum_{k=1}^r d_k$ for $0 \leq r \leq m$ (here $\sigma_0 := 0$) and

$$\alpha_r := \begin{cases} \infty & \text{for } r = 0 \\ \lceil \frac{\alpha}{d_r} \rceil & \text{for } 1 \leq r \leq m \\ 0 & \text{for } r = m+1 \end{cases}.$$

Define

$$e(\vec{f}; \alpha, r) := r\alpha + (n - \sigma_r) \cdot \begin{cases} \alpha_{r+1} & \text{if } \sigma_r \leq n \\ \alpha_r - 1 & \text{if } \sigma_r \geq n \end{cases}$$

and $e(\vec{f}; \alpha) := \min\{e(\vec{f}; \alpha, r) : r \in R(\vec{f}; \alpha)\}$ where

$$R(\vec{f}; \alpha) := \{0 \leq r \leq \min\{m, n-1\} : \alpha_{r+1} < \alpha_r\}$$

and

$$[\alpha]^{\delta(\vec{f}; \sigma)} := \begin{cases} \alpha & \text{if } n = \sigma_r \text{ for some } r \geq 1 \text{ and } r \in R(\vec{f}; \sigma) \\ 1 & \text{otherwise} \end{cases}.$$

The general version of Theorem 1.2 is as follows.

Theorem 1.5. *With the above setup, if p is a sufficiently large prime, depending on n and $\deg \vec{f}$, then*

$$(1.4) \quad \mathcal{N}(\vec{f}; p^\alpha) \ll_{n, \deg \vec{f}} [\alpha]^{\delta(\vec{f}; \sigma)} p^{-e(\vec{f}; \alpha)}$$

holds for all $\alpha \in \mathbb{N}$.

In many instances this theorem can also be shown to be sharp in the sense of Theorem 1.2; see the discussion in §3 for more details.

It is shown in §4 that the n -tuple of power sums (P_1, \dots, P_n) is non-degenerate over \mathbb{F}_p for all primes $p > n$. In this case $d_k = k$ and $\sigma_r = \Delta_r$, so that the exponent $e(\vec{f}; \alpha)$ in Theorem 1.5 reduces to the exponent $e_n(\alpha)$ appearing in Theorem 1.2. Thus, the upper bound in (1.1) is a consequence of (1.4).

The notion of non-degeneracy introduced above is very strong and it is natural to ask whether sharp bounds for $\mathcal{N}(\vec{f}; p^\alpha)$ can be established under weakened hypotheses. If one does not impose any kind of non-degeneracy condition, then this is a very difficult problem. Indeed, the simple case of

a single homogeneous polynomial in two variables was only recently understood [21]; the problem for a single homogeneous polynomial in n variables remains open and is closely related to certain long-standing conjectures of Igusa (see [12] and also [8]). Denef and Sperber [7] (see also [3, 4]) considered the case of a single homogeneous polynomial f in n variables under the hypothesis that f is *non-degenerate with respect to its Newton diagram* (see [7] for the relevant definitions). Although related, the present notion of non-degeneracy is somewhat different; for instance, $f(x, y, z) = (x-y)^2 + xz$ is non-degenerate in the sense of Definition 1.4 but it is not non-degenerate with respect to its Newton diagram. On the other hand, $f(x, y, z) = xyz$ is non-degenerate with respect to its Newton diagram yet it fails to satisfy the condition in Definition 1.4.

The introduction is concluded with a brief sketch of the methods used to prove Theorem 1.5. The problem can be lifted to the p -adic setting and reformulated as an estimate of the Haar measure of certain sub-level sets defined over \mathbb{Z}_p^n . An induction-on-scale procedure is then applied to determine the size of these sub-level sets. The base case and inductive step for this induction-on-scale can be loosely summarised as follows:

- The base case corresponds to studying the system

$$(1.5) \quad f_k(\vec{X}) \equiv 0 \pmod{p} \quad \text{for } 1 \leq k \leq m.$$

Upper and lower bounds on the number of solutions of such systems can be obtained by appealing to classical results from algebraic geometry, such as the Lang–Weil bound [17].

- To establish the inductive step one must verify certain transversality conditions which naturally arise in the analysis. This involves showing that certain configurations of hyperplanes in \mathbb{F}_p^n are in general position. Thus, the induction-on-scale effectively reduces a non-linear problem over rings with zero divisors to a linear algebra problem over finite fields.

This article is organised as follows: §2 and §3 contain the proof of Theorem 1.5. In particular, certain algebraic preliminaries are discussed in §2 whilst §3 contains the main details of the aforementioned induction argument. In §4 Theorem 1.5 is shown to imply the upper bound in Theorem 1.2. In §5 there is a detailed discussion of the lower bound in Theorem 1.2 and the $n = 3$ case. The paper concludes with an appendix which provides details of various facts from algebraic geometry and commutative algebra used to analyse the system (1.5).

2. Algebraic Preliminaries

Throughout this section let $1 \leq m \leq n$ and $\vec{f} := (f_1, \dots, f_m) \in \mathbb{Z}[X_1, \dots, X_n]$ be a system of homogeneous polynomials satisfying the non-degeneracy hypothesis over \mathbb{F}_p . The proofs of Theorem 1.2 and Theorem 1.5 will require estimates for the number of solutions to each of the partial systems of congruences

$$(2.1) \quad f_j(\vec{X}) \equiv 0 \pmod{p} \quad \text{for } 1 \leq j \leq r$$

for $1 \leq r \leq m$.

Lemma 2.1. *If $r = m = n$, then the system (2.1) has a unique (trivial) solution.*

Proof. If $\vec{x} \in \mathbb{F}_p^n$ satisfies $f_j(\vec{x}) \equiv 0 \pmod{p}$, then, by Euler's formula for homogeneous polynomials, $\langle \nabla f_j(\vec{x}), \vec{x} \rangle = 0$. Hence, the only solution to (2.1) for $r = n$ is $\vec{x} = \vec{0}$, since the non-degeneracy hypothesis implies that $\{\nabla f_j(\vec{x}) : 1 \leq j \leq n\}$ forms a basis of \mathbb{F}_p^n whenever $\vec{x} \neq \vec{0}$. \square

Counting the number of solutions to (2.1) when $r < n$ is more involved and is achieved by appealing to standard estimates from algebraic geometry. For this, it will be convenient to work over projective space. In particular, for $1 \leq r \leq m$ define

$$V_r := \{x \in \mathbb{P}^{n-1}(\overline{\mathbb{F}_p}) : f_j(x) = 0 \text{ for } 1 \leq j \leq r\}$$

and let $V_r(\mathbb{F}_p)$ denotes the set of \mathbb{F}_p -rational points of V_r ; here a point $x \in \mathbb{P}^{n-1}(\mathbb{F}_p)$ is \mathbb{F}_p -rational if it can be expressed in homogeneous coordinates as $x = [x_1 : \dots : x_n]$ with $x_1, \dots, x_n \in \mathbb{F}_p$.

Lemma 2.2 (Schwarz–Zippel-type bound). *For $1 \leq r \leq \min\{m, n-1\}$ one has*

$$|V_r(\mathbb{F}_p)| \leq \left(\prod_{j=1}^r \deg f_j \right) \cdot |\mathbb{P}^{n-r-1}(\mathbb{F}_p)|.$$

This lemma is a direct application of a well-known *Schwarz–Zippel-type bound*³ which applies to general projective varieties over \mathbb{F}_p : see, for instance, [16, Corollary 2.2]. To apply the Schwarz–Zippel bound one must demonstrate that each V_r is a projective variety of dimension $n - r - 1$; since V_r is defined by r homogeneous polynomial equations, given the non-degeneracy hypothesis it is intuitively clear that $\dim V_r = n - 1 - r$ should hold. However, the notion of dimension used here is of a precise algebraic-geometric nature and the verification of the condition $\dim V_r = n - 1 - r$ is postponed until the appendix.

³The terminology comes from comparison with the classical Schwarz–Zippel bound, which essentially corresponds to the case $m = 1$.

To establish the lower bound in Theorem 1.2 and the sharpness of the estimates in Theorem 1.5, one is also required to bound $|V_r(\mathbb{F}_p)|$ from below.

Proposition 2.3 (Lang–Weil estimate). *For $1 \leq r \leq \min\{m, n-2\}$ one has*

$$(2.2) \quad ||V_r(\mathbb{F}_p)| - |\mathbb{P}^{n-r-1}(\mathbb{F}_p)|| \ll_{\deg \vec{f}, n, r} p^{n-r-3/2}.$$

Proposition 2.3 is a direct application of the classical estimate of Lang–Weil [17]. In order to apply the Lang–Weil theorem, one must verify that the variety V_r is *absolutely irreducible*⁴ when $1 \leq r \leq n-2$; establishing this property requires some algebraic geometry and the proof is discussed in detail in the appendix. It is remarked that one may obtain stronger estimates by applying the deep work of Deligne [6]; here the Lang–Weil inequality is preferred due to its relative simplicity (in particular, there exist fairly elementary proofs of the Lang–Weil theorem: see [19, 2]).

Finally, it is remarked that for the prototypical example of (P_1, \dots, P_n) an upper bound on the number of solutions in \mathbb{F}_p^n can be obtained using very elementary methods.

Lemma 2.4. *For $1 \leq r \leq n$ one has*

$$\mathcal{N}(P_1, \dots, P_r; p) \leq n!p^{-r}.$$

Proof. Clearly one may write

$$\mathcal{N}(P_1, \dots, P_r; p) = \sum_{\vec{y}=(0, \dots, 0, y_{r+1}, \dots, y_n) \in \mathbb{F}_p^n} \mathcal{N}(\vec{P} - \vec{y}; p)$$

where $\vec{P} := (P_1, \dots, P_n)$. Observe that $\mathcal{N}(\vec{P} - \vec{y}; p)$ is a normalised count of n -tuples of roots of a fixed univariate polynomial over \mathbb{F}_p^n . One therefore immediately deduces that $\mathcal{N}(\vec{P} - \vec{y}; p) \leq n!p^{-n}$ and, since the above sum is over p^{n-r} choices of \vec{y} , this concludes the proof. \square

3. The proof of Theorem 1.5

The key observation in the proof of Theorem 1.5 is the following formula, which effectively reduces the problem to estimating the size of varieties over finite fields.

Proposition 3.1. *Let $n \in \mathbb{N}$ and p be prime. If $\vec{f} = (f_1, \dots, f_m)$ is non-degenerate over \mathbb{F}_p , then*

$$(3.1) \quad \mathcal{N}(\vec{f}; p^\alpha) \sim_{\deg \vec{f}} \sum_{r \in R(\vec{f}; \alpha)} c_n(\alpha, r) \cdot (\mathcal{N}(f_1, \dots, f_r; p) - p^{-n}) \cdot p^{-e(\vec{f}; \alpha, r) + r}$$

where $c_n(\alpha, r) = \alpha_r - \alpha_{r+1}$ if $\sigma_r = n$ and 1 otherwise.

⁴See the appendix for the relevant definitions.

Assuming this proposition, Theorem 1.5 readily follows from the estimates discussed in the previous section.

Proof (of Theorem 1.5). The Schwarz–Zippel-type bound (or, in the case of power sums, Lemma 2.4) from the previous section imply that

$$\mathcal{N}(f_1, \dots, f_r; p) \ll_{\deg \vec{f}, n, r} p^{-r} \quad \text{for } 1 \leq r \leq \min\{m, n-1\},$$

whilst Lemma 2.1 shows that $\mathcal{N}(f_1, \dots, f_n; p) = p^{-n}$. Applying these estimates to the formula (3.1), one immediately deduces that

$$\mathcal{N}(\vec{f}; p^\alpha) \ll_{\deg \vec{f}, n} [\alpha]^{\delta(\vec{f}; \sigma)} p^{-e(\vec{f}; \alpha)},$$

as required □

If p is sufficiently large depending on n and $\deg \vec{f}$, then Proposition 3.1 can be used to deduce effective lower bounds for $\mathcal{N}(\vec{f}; p^\alpha)$. A difficulty arises here due to the fact that the Lang–Weil estimate for $\mathcal{N}(f_1, \dots, f_r; p)$ is only available when $1 \leq r \leq n-2$. This causes complications if the minimum of $e(\vec{f}; \alpha, r)$ occurs when $r = n-1 \in R(\vec{f}; \alpha)$. In practice, this issue rarely manifests itself: in the prototypical case of the power sum system $\vec{f} = \vec{P}$ it only affects the $n = 3$ case, which can be understood completely via a direct counting argument (see §5).

To make the above discussion more concrete, suppose that $\vec{f} = (f_1, \dots, f_n)$ is non-degenerate over \mathbb{F}_p and the degrees d_k of the f_k satisfy $d_1 < \dots < d_n$. If α is sufficiently large, depending on $\deg \vec{f}$, then $\alpha_1 > \dots > \alpha_n$ and so $R(\vec{f}; \alpha) = \{0, 1, \dots, n-1\}$. As in the discussion following Theorem 1.2, one deduces that $e(\vec{f}; \alpha) = \min\{e(\vec{f}; \alpha, r_n^-), e(\vec{f}; \alpha, r_n^+)\}$ where

$$r_n^- := \max\{r \geq 0 : \sigma_r \leq n\} \quad \text{and} \quad r_n^+ := \min\{r \geq 0 : \sigma_r \geq n\}.$$

The Lang–Weil estimate (2.2) together with (3.1) therefore imply a sharp lower bound for $\mathcal{N}(\vec{f}; p^\alpha)$ whenever $1 \leq r_n^+ \leq n-2$. In the case $\vec{f} = \vec{P}$ is the power sum mapping, the condition $r_n^+ \leq n-2$ holds for all $n \geq 5$. On the other hand, the $n = 1, 2$ cases trivially admit sharp lower bounds whilst the remaining $n = 3, 4$ cases can be analysed via slightly more involved arguments (however, when $n = 3$ some anomalies arise: see §5).

The issue of the minimum of $e(\vec{f}; \alpha, r)$ occurring when $r = n-1 \in R(\vec{f}; \alpha)$ does not arise if the number of polynomial equations m satisfies $m \leq n-2$. An important case is given by $m = 1$ and $n \geq 3$, which treats a single non-degenerate (homogeneous) polynomial f of, say, degree d . Here $\alpha_1 = \lceil \frac{\alpha}{d} \rceil \geq 1$ so that $R(f; \alpha) = \{0, 1\}$. If $d \leq n$, then it is easy to see that $e(f; \alpha) = e(f; \alpha, 1) = \alpha$. On the other hand, if $n \leq d$ and one writes

$\alpha = (\alpha_1 - 1)d + j$ for some $1 \leq j \leq d$, then

$$e(f; \alpha) = \begin{cases} e(f; \alpha, 1) = (n/d)\alpha + j(1 - n/d) & \text{if } j \leq n \leq d \\ e(f; \alpha, 0) = n\alpha_1 & \text{if } n \leq j \leq d \end{cases}.$$

Hence Proposition 3.1 shows that, for p sufficiently large depending on d ,

$$\mathcal{N}(f; p^\alpha) \sim_d \begin{cases} p^{-\alpha} & \text{if } d < n \\ \alpha p^{-\alpha} & \text{if } d = n \\ p^{-((n/d)\alpha - j(n/d - 1))} & \text{if } j \leq n < d \\ p^{-n\alpha_1} & \text{if } n < d \text{ and } n \leq j \leq d \end{cases}.$$

This provides a precise count of the number of roots of f over $\mathbb{Z}/p^\alpha\mathbb{Z}$.

Proof (of Proposition 3.1). The solution count $\mathcal{N}(\vec{f}; p^\alpha)$ can be expressed as the Haar measure of a set over the p -adics via a simple lifting procedure. In particular, for $f \in \mathbb{Z}[X_1, \dots, X_n]$ and $l \in \mathbb{N}_0$ define the p -adic sub-level set

$$S(f, p^{-l}) := \{\vec{z} \in \mathbb{Z}_p^n : |f(\vec{z})| \leq p^{-l}\},$$

where $|\cdot|$ is the usual p -adic absolute value on \mathbb{Z}_p . It then follows that

$$(3.2) \quad \mathcal{N}(\vec{f}; p^\alpha) = \mu\left(\bigcap_{k=1}^m S(f_k, p^{-\alpha})\right),$$

where μ denotes the (normalised) Haar measure on the compact abelian group \mathbb{Z}_p^n . The space \mathbb{Z}_p^n is foliated into countably many concentric annuli⁵

$$\mathbb{A}_{p^{-l}}^n := \{\vec{z} \in \mathbb{Z}_p^n : |\vec{z}| := \max\{|z_1|, \dots, |z_n|\} = p^{-l}\}$$

so that

$$(3.3) \quad \begin{aligned} \mu\left(\bigcap_{k=1}^m S(f_k, p^{-\alpha})\right) &= \sum_{l \geq 0} \mu|_{\mathbb{A}_{p^{-l}}^n} \left(\bigcap_{k=1}^m S(f_k, p^{-\alpha})\right) \\ &= \sum_{l \geq 0} p^{-ln} \mu|_{\mathbb{A}_1^n} \left(\bigcap_{k=1}^m S(f_k, p^{-\alpha + ld_k})\right). \end{aligned}$$

Recall that α_r for $1 \leq r \leq m+1$ forms a sequence of non-increasing, non-negative integers. One may therefore write

$$(3.4) \quad \mu\left(\bigcap_{k=1}^m S(f_k, p^{-\alpha})\right) = \sum_{r=0}^m M_r = \sum_{r \in R(\vec{f}; \alpha)} M_r$$

where each M_r is of exactly the same form as the expression appearing on the right-hand side of (3.3) but with the summation in l restricted to the

⁵The basic decomposition found in the work [7] of Denef and Sperber is a foliation with respect to p -adic rectangles or boxes instead of concentric annuli. The notion of *non-degeneracy with respect to its Newton diagram* emerges naturally from such a decomposition whereas the present notion of non-degeneracy arises naturally from a concentric annuli decomposition.

range $\alpha_{r+1} \leq l < \alpha_r$. If $m \leq n-1$, then $R(\vec{f}; \alpha)$ is precisely the set of indices $0 \leq r \leq m$ for which the corresponding range of summation in M_r is non-empty. If $m = n$, then using Lemma 2.1 it is not difficult to see that $M_n = 0$, and thus the second equality in (3.4) is justified.

If $\alpha_{r+1} \leq l$ and $r+1 \leq k \leq m$, then $\alpha - ld_k \leq 0$ and, consequently, $S(f_k, p^{-\alpha+ld_k}) = \mathbb{Z}_p^n$. On the other hand, if $l < \alpha_r$ and $1 \leq k \leq r$, then $\alpha - ld_k \geq 1$. Combining these observations,

$$M_0 = \sum_{\alpha_1 \leq l} p^{-ln} \sim p^{-e(\vec{f}; \alpha, 0)}$$

and

$$M_r = \sum_{\alpha_{r+1} \leq l < \alpha_r} p^{-ln} \mu|_{\mathbb{A}_1^n} \left(\bigcap_{k=1}^r S(f_k, p^{-\alpha+ld_k}) \right)$$

for $1 \leq r \leq m$, where each of the exponents $\alpha - ld_k$ appearing in the above expression is at least 1.

Lemma 3.2. *The identity*

$$(3.5) \quad \mu|_{\mathbb{A}_1^n} \left(\bigcap_{k=1}^r S(f_k, p^{-l_k}) \right) = (\mathcal{N}(f_1, \dots, f_r; p) - p^{-n}) \cdot p^{-\sum_{k=1}^r l_k + r}$$

holds for all $1 \leq r \leq m$ and $l_1 \geq \dots \geq l_r \geq 1$.

Temporarily assuming this lemma and letting $1 \leq r \leq m$ with $r \in R(\vec{f}; \alpha)$, one obtains the identity

$$M_r = (\mathcal{N}(f_1, \dots, f_r; p) - p^{-n}) \cdot p^{-r\alpha+r} \sum_{\alpha_{r+1} \leq l < \alpha_r} p^{-l(n-\sigma_r)}.$$

A simple computation shows that

$$\sum_{\alpha_{r+1} \leq l < \alpha_r} p^{-l(n-\sigma_r)} \sim c_n(\alpha, r) \cdot \begin{cases} p^{-(n-\sigma_r)\alpha_{r+1}} & \text{if } \sigma_r \leq n \\ p^{-(n-\sigma_r)(\alpha_r-1)} & \text{if } \sigma_r \geq n \end{cases}$$

where $c_n(\alpha, r) = \alpha_r - \alpha_{r+1}$ if $\sigma_r = n$ and 1 otherwise. Substituting these estimates into the formula for M_r , it follows that

$$(3.6) \quad M_r \sim c_n(\alpha, r) \cdot (\mathcal{N}(f_1, \dots, f_r; p) - p^{-n}) \cdot p^{-e(\vec{f}; \alpha, r) + r}$$

holds for the exponent $e(\vec{f}; \alpha, r)$ from the introduction. Combining (3.2), (3.4) and (3.6), one obtains the desired formula. \square

Proof (of Lemma 3.2). The proof proceeds by inducting on l_1 . If $l_1 = 1$, then $l_1 = \dots = l_r = 1$ and the left-hand side of (3.5) can be written as

$$p^{-n} \# \{ \vec{z} \in \mathbb{F}_p^n \setminus \{ \vec{0} \} : f_k(\vec{z}) \equiv 0 \pmod{p} \text{ for } 1 \leq k \leq r \} = \mathcal{N}(f_1, \dots, f_r; p) - p^{-n},$$

as required.

Now suppose $l_1 \geq 2$ and that the estimate is valid for all smaller values of l_1 . The left-hand side of (3.5) can be expressed as

$$(3.7) \quad \sum_{\vec{u} \in [\mathbb{Z}/p^{l_1-1}\mathbb{Z}]^n : |\vec{u}|=1} p^{-(l_1-1)n} \mu \left(\bigcap_{k=1}^r S(f_k(\vec{u} + p^{l_1-1} \cdot), p^{-l_k}) \right).$$

For $1 \leq k \leq r$ one has

$$(3.8) \quad f_k(\vec{u} + p^{l_1-1} \vec{z}) \equiv f_k(\vec{u}) + p^{l_1-1} \nabla f_k(\vec{u}) \cdot \vec{z} \pmod{p^{l_k}},$$

which follows from Taylor's theorem and the fact that $2(l_1 - 1) \geq l_1 \geq l_k$. Let $1 \leq s \leq r$ be the largest integer such that $l_1 = \dots = l_s$. As a consequence of the identity (3.8), if $1 \leq k \leq s$ and $|f_k(\vec{u} + p^{l_1-1} \vec{z})| \leq p^{-l_k}$ for some $\vec{z} \in \mathbb{Z}_p^{n-1}$, then $|f_k(\vec{u})| \leq p^{-(l_k-1)}$. On the other hand, if $s+1 \leq k \leq r$, then $f_k(\vec{u} + p^{l_1-1} \vec{z}) \equiv f_k(\vec{u}) \pmod{p^{l_k}}$ for all $\vec{z} \in \mathbb{Z}_p^{n-1}$. Define

$$\tilde{l}_k := \begin{cases} l_k - 1 & \text{for } 1 \leq k \leq s \\ l_k & \text{for } s+1 \leq k \leq r \end{cases},$$

noting that $\tilde{l}_k \geq 1$ for $1 \leq k \leq r$. For $\vec{u} \in \mathbb{Z}_p^n$ with $|f_k(\vec{u})| \leq p^{-\tilde{l}_1}$ let $L_{k,\vec{u}}$ denote the degree 1 polynomial

$$L_{k,\vec{u}}(\vec{z}) := p^{-\tilde{l}_1} f_k(\vec{u}) + \nabla f_k(\vec{u}) \cdot \vec{z}.$$

Combining the above observations, (3.7) can be written as

$$(3.9) \quad \sum_{\substack{\vec{u} \in [\mathbb{Z}/p^{\tilde{l}_1}\mathbb{Z}]^n : |\vec{u}|=1 \\ |f_k(\vec{u})| \leq p^{-\tilde{l}_k} \text{ for } 1 \leq k \leq r}} p^{-\tilde{l}_1 n} \mu \left(\bigcap_{k=1}^s S(L_{k,\vec{u}}, p^{-1}) \right).$$

Thus the problem is reduced to estimating the size of intersections of neighbourhoods of certain hyperplanes in \mathbb{Z}_p^n .

Lemma 3.3. *If $\vec{u} \in \mathbb{A}_1^n$ satisfies $|f_k(\vec{u})| \leq p^{-1}$ for $1 \leq k \leq r$, then*

$$(3.10) \quad \mu \left(\bigcap_{k=1}^s S(L_{k,\vec{u}}, p^{-1}) \right) = p^{-s}$$

for $1 \leq s \leq r$.

Applying this identity to (3.9) one observes that (3.7) can be written as

$$p^{-s-\tilde{l}_1 n} \# \{ \vec{u} \in [\mathbb{Z}/p^{\tilde{l}_1}\mathbb{Z}]^n : |\vec{u}| = 1 \text{ and } f_k(\vec{u}) \equiv 0 \pmod{p^{\tilde{l}_k}} \text{ for } 1 \leq k \leq r \},$$

which can then be expressed as the p -adic integral

$$p^{-s} \mu|_{\mathbb{A}_1^n} \left(\bigcap_{k=1}^r S(f_k, p^{-\tilde{l}_k}) \right).$$

The induction hypothesis, coupled with the identity

$$s + \sum_{k=1}^r \tilde{l}_k = \sum_{k=1}^r l_k,$$

now implies that

$$p^{-s} \mu|_{\mathbb{A}_1^n} \left(\bigcap_{k=1}^r S(f_k, p^{-\tilde{l}_k}) \right) = (\mathcal{N}(f_1, \dots, f_r; p) - p^{-n}) \cdot p^{-\sum_{k=1}^r l_k + r}$$

Combining the preceding chain of identities closes the induction and concludes the proof of Lemma 3.2. \square

It remains to prove Lemma 3.3.

Proof (of Lemma 3.3). Given $\vec{u} \in \mathbb{Z}_p^n$ satisfying the hypotheses of the lemma, one wishes to study the intersection properties of the sets

$$S(L_{\vec{u},k}, p^{-1}) = \{\vec{z} \in \mathbb{Z}_p^n : |p^{-l_1+1} f_k(\vec{u}) + \nabla f_k(\vec{u}) \cdot \vec{z}| \leq p^{-1}\}.$$

The non-degeneracy hypothesis implies that $\nabla f_k(\vec{u}) \not\equiv 0 \pmod{p}$ for $1 \leq k \leq r$, and so each $S(L_{\vec{u},k}, p^{-1})$ is a p^{-1} -neighbourhood of a hyperplane in \mathbb{Z}_p^n . The size of the intersection of the $S(L_{\vec{u},k}, p^{-1})$ for $1 \leq k \leq s$ is therefore governed by angles between the normal vectors $\nabla f_1(\vec{u}), \dots, \nabla f_s(\vec{u})$. More precisely, the non-degeneracy hypothesis implies the existence of some $\mathbf{j} = (j_1, \dots, j_{n-s}) \in \{1, \dots, n\}^{n-s}$ such that

$$|\det(\nabla f_1(\vec{u}) \quad \dots \quad \nabla f_s(\vec{u}) \quad e_{j_1} \quad \dots \quad e_{j_{n-s}})| = 1,$$

where the e_j are the standard basis vectors. Expressing the left-hand side of (3.10) as

$$\int_{\mathbb{Z}_p^n} \prod_{k=1}^s \chi_{B(0,p^{-1})}(p^{-l_1+1} f_k(\vec{u}) + \nabla f_k(\vec{u}) \cdot \vec{z}) d\mu(\vec{z}),$$

it follows from the p -adic change of variables formula (see, for instance, [13, §7.5]), that

$$\mu \left(\bigcap_{k=1}^s S(L_{\vec{u},k}, p^{-1}) \right) = \int_{\mathbb{Z}_p^s} \prod_{k=1}^s \chi_{B(0,p^{-1})}(y_k) d\mu(\vec{y}) = p^{-s},$$

as required. \square

4. Applying Theorem 1.5 to count factorisations of monomials

In order to apply Theorem 1.5 to the problem of factorising monomials, one must verify that the system of power sums satisfies the non-degeneracy hypothesis.

Lemma 4.1. *If $P_k \in \mathbb{Z}[X_1, \dots, X_n]$ denotes the k -th power sum, then $\vec{P} := (P_1, \dots, P_n)$ is non-degenerate over \mathbb{F}_p for all primes $p > n$.*

Proof. Fixing $1 \leq r \leq n$, suppose that $\vec{z} \in \overline{\mathbb{F}}_p^n$ satisfies

$$P_k(\vec{z}) = 0 \quad \text{for } 1 \leq k \leq r$$

and that the vectors $\nabla P_1(\vec{z}), \dots, \nabla P_r(\vec{z})$ are linearly dependent in $\overline{\mathbb{F}}_p^n$. If $\mathbf{k} = (k_1, \dots, k_r) \in \mathbb{N}^r$ with $1 \leq k_1 < \dots < k_r \leq n$, then it follows that

$$(4.1) \quad \det(\nabla^{\mathbf{k}} P_1(\vec{z}) \quad \dots \quad \nabla^{\mathbf{k}} P_r(\vec{z})) = 0,$$

where $\nabla^{\mathbf{k}}: \mathbb{Z}[X_1, \dots, X_n] \mapsto \mathbb{Z}[X_1, \dots, X_n]^r$ is the differential operator

$$\nabla^{\mathbf{k}} f := (\partial_{x_{k_1}} f, \dots, \partial_{x_{k_r}} f).$$

The determinant in (4.1) is given by

$$r! \prod_{1 \leq i < j \leq r} (z_{k_i} - z_{k_j})$$

where, by the hypothesis $p > n$, $r! \not\equiv 0 \pmod{p}$. Combining these observations, it follows that the z_1, \dots, z_n assume at most $r - 1$ values in $\overline{\mathbb{F}}_p^n$. In particular, there exists a partition A_1, \dots, A_t of $\{1, \dots, n\}$ into at most $r - 1$ non-empty sets and a collection of distinct elements $x_i \in \overline{\mathbb{F}}_p$ such that

$$z_k = x_i \quad \text{whenever } k \in A_i.$$

Thus, if $a_i = \#A_i$, then $(x_1, \dots, x_t) \in \overline{\mathbb{F}}_p^t$ is a solution to the square system

$$(4.2) \quad \sum_{i=1}^t a_i X_i^k = 0 \quad \text{for } 1 \leq k \leq t.$$

For any non-empty $S \subseteq \{1, \dots, t\}$ it follows that $1 \leq \sum_{i \in S} a_i \leq n$ and so $p \nmid \sum_{i \in S} a_i$. It is shown in Proposition 4.2 below that, under these hypotheses, only the trivial solution satisfies a system of the form (4.2), and one therefore deduces that $z_k = 0$ for $1 \leq k \leq n$. This shows the system $\vec{P} = (P_1, \dots, P_n)$ is non-degenerate over \mathbb{F}_p . \square

The above argument relied upon the following proposition.

Proposition 4.2. *Let R be an integral domain, $\vec{a} = (a_1, \dots, a_n) \in R^n$ and define the weighted power sums*

$$P_{\vec{a},k}(X_1, \dots, X_n) := \sum_{i=1}^n a_i X_i^k \quad \text{for } 1 \leq k \leq n.$$

If $\sum_{i \in S} a_i \neq 0$ for all non-empty $S \subseteq \{1, \dots, n\}$, then the system

$$(4.3) \quad P_{\vec{a},k}(X_1, \dots, X_n) = 0 \quad \text{for } 1 \leq k \leq n$$

has a unique (trivial) solution in R^n .

The proposition is a consequence of the following identity (see [14, Theorem 4.3] for an alternative approach).

Lemma 4.3 (Weighted Newton–Girard formula). *If R is commutative ring (with identity) and $\vec{a} = (a_1, \dots, a_n) \in R^n$, then*

$$(4.4) \quad \left(\sum_{i=1}^n a_i \right) e_n(X_1, \dots, X_n) = \sum_{k=1}^n (-1)^{k-1} e_{n-k}(X_1, \dots, X_n) P_{\vec{a}, k}(X_1, \dots, X_n),$$

where the $e_k \in R[X_1, \dots, X_n]$ are the elementary symmetric polynomials in n variables.

Proof. Observe that

$$e_{n-k}(X_1, \dots, X_n) = X_i e_{n-(k+1)}(X_1, \dots, \hat{X}_i, \dots, X_n) + e_{n-k}(X_1, \dots, \hat{X}_i, \dots, X_n)$$

for $1 \leq i, k \leq n$, where the notation \hat{X}_i is used to signify the omission of the X_i variable. Here e_{-1} is interpreted as the zero polynomial (and e_0 is the constant polynomial 1). Using this identity, one may express the right-hand side of (4.4) as

$$\sum_{i=1}^n a_i \sum_{k=1}^n (-1)^{k-1} (X_i^{k+1} e_{n-(k+1)}(X_1, \dots, \hat{X}_i, \dots, X_n) + X_i^k e_{n-k}(X_1, \dots, \hat{X}_i, \dots, X_n)).$$

Each sum in the k index is telescoping and it is easy to see that the above expression reduces to

$$\sum_{i=1}^n a_i X_i e_{n-1}(X_1, \dots, \hat{X}_i, \dots, X_n) = \left(\sum_{i=1}^n a_i \right) e_n(X_1, \dots, X_n),$$

as required. \square

The proposition is now immediate.

Proof (of Proposition 4.2). The proof is by induction on n , the case $n = 1$ being vacuous. Suppose that $\vec{x} = (x_1, \dots, x_n) \in R^n$ is a solution to (4.3). By Lemma 4.3 one has

$$\left(\sum_{i=1}^n a_i \right) x_1 \dots x_n = 0$$

and, since by hypothesis $\sum_{i=1}^n a_i \neq 0$ and R is an integral domain, one deduces that $x_i = 0$ for some $1 \leq i \leq n$. Without loss of generality suppose that $x_n = 0$. Then $(x_1, \dots, x_{n-1}) \in R^{n-1}$ is a solution to the system

$$P_{\vec{a}', k}(X_1, \dots, X_{n-1}) = 0 \quad \text{for } 1 \leq k \leq n-1$$

where the coefficient vector $\vec{a}' := (a_1, \dots, a_{n-1})$ automatically satisfies the hypothesis of the proposition. Thus, by the induction hypothesis, $x_i = 0$ for $1 \leq i \leq n-1$, as required. \square

5. Lower bounds in Theorem 1.2

As already noted, the upper bounds in Theorem 1.2 follow from Theorem 1.5. A slightly more refined analysis is needed to complete the proof of the asymptotic formula (1.1) in Theorem 1.2 for all degrees $n \neq 3$. In particular, it is now shown that for all sufficiently large primes p the inequality

$$(5.1) \quad \mathbf{N}(\vec{0}_n; p^\alpha) \gg_n [\alpha]^{\delta_n(\Delta)} p^{-e_n(\alpha)}$$

holds for all $\alpha \in \mathbb{N}$ and $n \neq 3$. As by-product of analysis, the sharp result in the $n = 3$ case may also be derived, which curiously has additional dependence on both the parity of α and the congruence class of p modulo 3.

Recall the key formula

$$(5.2) \quad \mathbf{N}(\vec{0}_n; p^\alpha) \sim_n \sum_{r \in R_n(\alpha)} c_n(\alpha, r) \cdot (\mathcal{N}(P_1, \dots, P_r; p) - p^{-n}) \cdot p^{-e_n(\alpha, r) + r}$$

established in Proposition 3.1. First suppose that $n = \Delta_{r'}$ for some $r' \geq 2$ and that $r' \in R_n(\alpha)$ so that $[\alpha]^{\delta_n(\Delta)} = \alpha$. In this case, $c_n(\alpha, r') \sim_n \alpha$ and $c_n(\alpha, r) = 1$ for all other values of r . If $n \neq 3$, then $r' \leq n - 2$ and so the Lang–Weil bound (2.2) yields

$$(5.3) \quad \mathcal{N}(P_1, \dots, P_r; p) \gg_n p^{-r}.$$

for $r = r'$. The lower bound (5.1) now follows by combining (5.3) with (5.2). Thus, provided $n \neq 3$, one may assume without loss of generality that $[\alpha]^{\delta_n(\Delta)} = 1$ and $c_n(\alpha, r) = 1$ for all α and r .

Focusing on the $n \neq 3$ case, it now suffices to show that for $n \neq 3$ the estimate

$$(5.4) \quad \mathbf{N}(\vec{0}_n; p^\alpha) \gg_n p^{-e_n(\alpha)}$$

holds for all $\alpha \in \mathbb{N}$. By (5.2), this would follow if one could demonstrate that there exists some $r \in R_n(\alpha)$ for which $e_n(\alpha) = e_n(\alpha, r)$ and (5.3) holds.

Low degree case. For any value of $n \in \mathbb{N}$ it is immediate that

$$(5.5) \quad \mathcal{N}(\emptyset; p) = 1 \quad \text{and} \quad \mathcal{N}(P_1; p) = p^{-1}.$$

From these identities it follows that (5.1) holds, establishing Theorem 1.2 for $n = 1, 2$.

High degree case. Here (5.4) is established for degrees $n \geq 4$. Recall that the Lang–Weil estimate (2.2) implies that (5.3) holds for all $1 \leq r \leq n - 2$ and, trivially, (5.3) is also valid for $r = n$. Thus, if either $n - 1 \notin R_n(\alpha)$ or there exists some $1 \leq r \leq n - 2$ with $r \in R_n(\alpha)$ and $e_n(\alpha, n - 1) \geq e_n(\alpha, r)$, then the desired lower bound (5.4) immediately follows.

These observations allow one to easily treat the $n = 4$ case. It is useful to first compute the relevant exponents:

$$\begin{aligned} e_4(\alpha, 0) &= 4\alpha, & e_4(\alpha, 1) &= \alpha + 3\lceil \frac{\alpha}{2} \rceil, \\ e_4(\alpha, 2) &= 2\alpha + \lceil \frac{\alpha}{3} \rceil, & e_4(\alpha, 3) &= 3\alpha - 2\lceil \frac{\alpha}{3} \rceil + 2. \end{aligned}$$

Since $e_4(\alpha, 2) \leq e_4(\alpha, 3)$, the lower bound (5.4) holds whenever $2 \in R_4(\alpha)$ or $3 \notin R_4(\alpha)$. This leaves only $\alpha = 4$, but since $e_4(4, 1) = e_4(4, 3) = 10$, the result also holds in this case.

A similar, but more involved, argument allows one to treat $n \geq 5$. Let $n \geq 5$ and suppose, aiming for a contradiction, that $n-1 \in R_n(\alpha)$ and that there exists no value of $r \in R_n(\alpha)$ with $1 \leq r \leq n-2$ and $e_n(\alpha, n-1) \geq e_n(\alpha, r)$. Recall from the introduction that

$$e_n(\alpha, r+1) - e_n(\alpha, r) \geq 1 \quad \text{for } \Delta_r \geq n.$$

It therefore follows that $r \notin R_n(\alpha)$ for $r_n^+ \leq r \leq n-2$ and so

$$k := \left\lceil \frac{\alpha}{r_n^+} \right\rceil = \left\lceil \frac{\alpha}{n-1} \right\rceil.$$

In particular,

$$(5.6) \quad \alpha = (k-1)(n-1) + j = (k-1)r_n^+ + j'$$

for some $1 \leq j \leq n-1$ and $1 \leq j' \leq r_n^+$.

If $k = 1$, then $\lceil \frac{\alpha}{n-1} \rceil = 1 = \lceil \frac{\alpha}{n} \rceil$, contradicting the assumption that $n-1 \in R_n(\alpha)$. If $j' = r_n^+$, then

$$\frac{\alpha}{r_n^+} = \left\lceil \frac{\alpha}{r_n^+} \right\rceil < \left\lceil \frac{\alpha}{r_n^+ - 1} \right\rceil$$

and so $r_n^+ - 1 \in R_n(\alpha)$. Furthermore,

$$\begin{aligned} e_n(\alpha, r_n^+) - e_n(\alpha, r_n^+ - 1) &= \alpha + (n - \Delta_{r_n^+})(\lceil \frac{\alpha}{r_n^+} \rceil - 1) - (n - \Delta_{r_n^+ - 1})\lceil \frac{\alpha}{r_n^+} \rceil \\ &= \alpha - r_n^+ \cdot \lceil \frac{\alpha}{r_n^+} \rceil + (\Delta_{r_n^+} - n) = \Delta_{r_n^+} - n \geq 0, \end{aligned}$$

which implies that $e_n(\alpha, n-1) \geq e_n(\alpha, r_n^+ - 1)$, a contradiction.

The above observations show that $k \geq 2$ and $1 \leq j' \leq r_n^+ - 1$ and so (5.6) yields

$$(k-1)(n-1-r_n^+) = j' - j \leq r_n^+ - 2.$$

Write $n = \Delta_{r_n^+ - 1} + s_n$ for some $1 \leq s_n \leq r_n^+$ so that

$$(k-1)(r_n^+(r_n^+ - 3) + 2(s_n - 1)) \leq 2r_n^+ - 4.$$

If $k \geq 3$ and $s_n \geq 2$, then r_n^+ must satisfy

$$(x-2)^2 = x^2 - 4x + 4 \leq 0$$

which forces $r_n^+ = 2$ and hence $n = 3$, but this contradicts the assumption $n \geq 5$. Furthermore, if $k \geq 3$ and $s_n = 1$, then r_n^+ must satisfy $x^2 - 4x + 2 \leq$

| n | r_n^+ | s_n | t_n |
|-----|---------|-------|-------|
| 5 | 3 | 2 | 0 |
| 6 | 3 | 3 | 2 |
| 7 | 4 | 1 | 0 |
| 8 | 4 | 2 | 2 |
| 9 | 4 | 3 | 4 |
| 10 | 4 | 4 | 6 |

FIGURE 1. If $n \geq 5$, then $t_n \leq 0$ holds only for $n = 5$ and $n = 7$.

0. This implies that $r_n^+ \in \{2, 3\}$ and so $3 \leq n \leq 6$; of these values of n , only $n = 4$ satisfies $s_n = 1$, again contradicting the assumption that $n \geq 5$.

From the preceding analysis one deduces that $k = 2$ and that n must satisfy the inequality

$$(5.7) \quad t_n := (r_n^+)^2 - 5r_n^+ + 2(s_n + 1) \leq 0.$$

Again using the basic estimate $s_n \geq 1$, it follows that $r_n^+ \leq 4$ and so $5 \leq n \leq 10$. Furthermore, an explicit computation (see Figure 1) now shows that 5 and 7 are the only values of n for which (5.7) holds. For both $n = 5$ and $n = 7$ the inequality (5.7) is saturated. Consequently, j must assume the extreme value $j = 1$ and so $\alpha = n$. Finally, by direct computation one may show that $2 \in R_5(5)$, $3 \in R_7(7)$ and

$$e_5(5, 2) = 14 \leq e_5(5, 4) = 15, \quad e_7(7, 3) = 23 \leq e_7(7, 6) = 28,$$

which is the desired contradiction.

Intermediate degree ($n = 3$) case. It remains to examine the situation when $n = 3$, which is a little more complicated.

Given $\vec{a} = (a_1, \dots, a_r) \in \mathbb{Z}$ define $f_{\vec{a}}(x) := \sum_{j=1}^r a_j x^j$. For any $n \in \mathbb{N}$ the basic properties of character sums imply that

$$\begin{aligned} \mathcal{N}(P_1, \dots, P_r; p) &= p^{-n-r} \sum_{a_1(p)} \dots \sum_{a_r(p)} \left(\sum_{x(p)} e^{2\pi i f_{\vec{a}}(x)/p} \right)^n \\ &= p^{-r} + p^{-r} \sum_{\vec{a}(p) : \vec{a} \not\equiv \vec{0} \pmod{p}} \left(p^{-1} \sum_{x(p)} e^{2\pi i f_{\vec{a}}(x)/p} \right)^n, \end{aligned}$$

where the sums in x and the a_j in the first line are each over a complete set of residues modulo p . If $r = 2$ and p is odd, then the above expression involves classical Gauss sums which can be evaluated using the formula

$$(5.8) \quad p^{-1} \sum_{x(p)} e^{2\pi i (ax^2 + bx)/p} = \varepsilon_p(a|p) p^{-1/2} e^{-2\pi i (4a)^{-1} b^2/p} \quad \text{for } a \not\equiv 0 \pmod{p}.$$

Here $\varepsilon_p = 1$ whenever $p \equiv 1 \pmod{4}$ and $\varepsilon_p = i$ otherwise, and $(a|p)$ is the Legendre symbol. Indeed, by completing the square in the phase, (5.8) is a direct consequence of Gauss' classical formula for quadratic Gauss sums (see, for instance, [1, §9.10]). Writing $\mathcal{N}(P_1, P_2; p) = p^{-2} + E$, it follows from the above identity that

$$E = \varepsilon_p^n p^{-(n+4)/2} \sum_{a \pmod{p}: a \not\equiv 0 \pmod{p}} (a|p)^n \sum_{b \pmod{p}} e^{-2\pi i n(4a)^{-1} b^2/p}.$$

The sum in b can also be evaluated and, applying elementary properties of quadratic residues (in particular, the completely multiplicative property of the Legendre symbol), one obtains

$$E = \varepsilon_p^{n+1} (-n|p) p^{-(n+3)/2} \sum_{a \pmod{p}: a \not\equiv 0 \pmod{p}} (a|p)^{n-1}.$$

Recall that there are precisely $(p-1)/2$ non-zero quadratic residues and $(p-1)/2$ quadratic non-residues modulo p . Thus,

$$\sum_{a \pmod{p}: a \not\equiv 0 \pmod{p}} (a|p)^{n-1} = (1 + (-1)^{n-1}) \cdot \frac{p-1}{2}$$

and, consequently,

$$(5.9) \quad E = \begin{cases} 0 & \text{if } n \text{ is even} \\ \varepsilon_p^{n+1} (-n|p) p^{-(n+3)/2} (p-1) & \text{if } n \text{ is odd} \end{cases}.$$

The above formula can be used to treat the $n = 3$ case, which behaves in a distinctly different manner from that of every other degree. Here the relevant exponents are given by

$$e_3(\alpha, 0) = 3\alpha, \quad e_3(\alpha, 1) = \alpha + 2\left\lceil \frac{\alpha}{2} \right\rceil, \quad e_3(\alpha, 2) = 2\alpha.$$

If $2 \notin R_3(\alpha)$ (that is, $\alpha \in \{1, 2, 4\}$), then the bound

$$(5.10) \quad \mathbf{N}(\vec{0}_3; p^\alpha) \gg [\alpha]^{\delta_3(\Delta)} p^{-e_3(\alpha)}$$

follows immediately from the trivial identities stated in (5.5) (note that, in this case, $[\alpha]^{\delta_n(\Delta)} = 1$). If $2 \in R_3(\alpha)$, then the analysis is more complex. The identity (5.9) implies that⁶

$$\mathcal{N}(P_1, P_2; p) = \begin{cases} 2p^{-2} - p^{-3} & \text{if } -3 \text{ is a quadratic residue modulo } p \\ p^{-3} & \text{otherwise} \end{cases}.$$

By the law of quadratic reciprocity, -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{3}$. Thus, if $2 \in R_3(\alpha)$ and $p \equiv 1 \pmod{3}$, then (5.10) once again holds. Now suppose that $2 \in R_3(\alpha)$ and $p \not\equiv 1 \pmod{3}$. If α is even, then $e_3(\alpha, 1) = e_3(\alpha, 2) = 2\alpha$ and so

$$\mathbf{N}(\vec{0}_3; p^\alpha) \sim p^{-e_3(\alpha)},$$

⁶Here it is assumed that $p > 3$ so that $(-3|p) \neq 0$.

by (5.2), which differs by a logarithm from what one would expect based on the bounds for $n \neq 3$. If α is odd, then $e_3(\alpha, 1) = e_3(\alpha, 2) + 1$ and so

$$\mathbf{N}(\vec{0}_3; p^\alpha) \sim p^{-e_3(\alpha)-1}$$

again by (5.2), which differs by a factor of p^{-1} (up to a logarithmic factor) from what one would expect based on the bounds for $n \neq 3$. The situation for $n = 3$ is therefore summarised as follows.

Lemma 5.1. *If p is a sufficiently large prime, then*

$$\mathbf{N}(\vec{0}_3; p^\alpha) \sim [\alpha]^{\delta_3(\Delta) \cdot \kappa(p)} p^{-e_3(\alpha) - \lambda(\alpha) \cdot (1 - \kappa(p))}$$

holds for all $\alpha \in \mathbb{N}$ where

$$\lambda(\alpha) := \begin{cases} 1 & \text{if } \alpha > 1 \text{ is odd} \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \kappa(p) := \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3} \\ 0 & \text{otherwise} \end{cases}.$$

Thus, Lemma 5.1 and Theorem 1.2 provide a precise count of the number of factorisations of X^n over $\mathbb{Z}/p^\alpha\mathbb{Z}$ for all degrees n , provided the prime p is sufficiently large.

Appendix A. Irreducibility of projective varieties defined by non-degenerate systems

Recall that the Lang–Weil theorem [17] was used to derive Proposition 2.3, which formed the base case of the induction argument used to prove Theorem 1.5. To justify the application of the Lang–Weil bound, one must verify that certain projective varieties defined by the homogenous polynomials f_k are *absolutely irreducible*: that is, they are irreducible as varieties over $\mathbb{P}^{n-1}(\overline{\mathbb{F}}_p)$.

Lemma A.1. *Suppose $1 \leq m \leq n-2$ and $\vec{f} := (f_1, \dots, f_m)$ is a system of homogeneous polynomials that satisfies the non-degeneracy hypothesis. The projective variety*

$$(A.1) \quad V := \{x \in \mathbb{P}^{n-1}(\overline{\mathbb{F}}_p) : f_j(x) = 0 \text{ for } 1 \leq j \leq m\}$$

is irreducible.

As a consequence of the proof of Lemma A.1, one can also verify the dimension condition needed for the application of the Schwarz–Zippel bound in Lemma 2.2.

Corollary A.2. *Suppose $1 \leq m \leq n-1$ and $\vec{f} := (f_1, \dots, f_m)$ is a system of homogeneous polynomials that satisfies the non-degeneracy hypothesis. If V is as in (A.1), then $\dim V = n-1-m$.*

Before stating the proof of Lemma A.1 and Corollary A.2, it is useful to review some of the basic concepts from commutative algebra and algebraic

geometry which appear in the argument. All the facts and definitions presented below are standard and can be found in many textbooks (see, for instance, [15]).

Let K be an algebraically closed field and R be a commutative, Noetherian ring (for instance, $R = K[X_1, \dots, X_n]$).

- A projective variety $V \subseteq \mathbb{P}^{n-1}(K)$ is the zero-locus of a set $f_1, \dots, f_r \in K[X_1, \dots, X_n]$ of homogeneous polynomials (note that here a variety is *not* required to be irreducible). If, in particular, $V = \{x \in \mathbb{P}^{n-1}(K) : f(x) = 0\}$ is the zero-locus of a single non-constant homogeneous polynomial $f \in K[X_1, \dots, X_n]$, then V is said to be a projective hypersurface.
- The ideal $\mathcal{I}(V)$ of a variety $V \subseteq \mathbb{P}^{n-1}(K)$ is the collection of all polynomials in $K[X_1, \dots, X_n]$ which vanish on V . Fixing homogeneous polynomials $f_1, \dots, f_r \in K[X_1, \dots, X_n]$ and defining

$$V := \{x \in \mathbb{P}^{n-1}(K) : f_j(x) = 0 \text{ for all } 1 \leq j \leq r\},$$

if $I := \langle f_1, \dots, f_r \rangle$ denotes the homogeneous ideal generated by the f_1, \dots, f_r , then Hilbert's Nullstellensatz states that

$$\mathcal{I}(V) = \sqrt{I}.$$

Here, for any ideal $I \subseteq R$, the radical ideal \sqrt{I} is defined by

$$\sqrt{I} := \{f \in R : f^m \in I \text{ for some } m \in \mathbb{N}\}$$

- A projective variety $V \subseteq \mathbb{P}^{n-1}(K)$ is irreducible if the following holds: if $V = V_1 \cup V_2$ for $V_1, V_2 \subseteq \mathbb{P}^{n-1}$ projective varieties, then $V_1 = V$ or $V_2 = V$. This condition is equivalent to the primality of the ideal $\mathcal{I}(V)$.
- A chain of prime ideals of the form $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_k$ is said to have length k (here each $\mathfrak{p}_j \subseteq R$ is a prime ideal and the inclusions are strict). The Krull dimension of a ring R , which is denoted by $\dim R$, is the supremum of all lengths of chains of prime ideals in R . As a key example, $\dim K[X_1, \dots, X_n] = n$; in fact the length of *any* maximal chain of prime ideals in $K[X_1, \dots, X_n]$ is n (see, for instance, [15, Chapter II, Proposition 3.4]).
- Given a prime ideal $\mathfrak{p} \subseteq R$ define the height of \mathfrak{p} to be the supremum of all lengths of prime ideals of R contained in \mathfrak{p} . The height of an arbitrary (that is, not necessarily prime) proper ideal $I \subseteq R$, which is denoted $\text{height}(I)$, is then defined to be the infimum of the heights of all prime ideals which contain I . Since any prime ideal containing I automatically contains \sqrt{I} , it follows that $\text{height}(\sqrt{I}) = \text{height}(I)$. The generalised Krull principal ideal theorem (see, for instance, [15, Chapter V, Theorem 3.4]) asserts that if $I = \langle f_1, \dots, f_r \rangle$ is generated by r elements, then $\text{height}(I) \leq r$.

- The dimension $\dim V$ of a projective variety V is given by $\dim V := \dim K[V] - 1$ where $K[V]$ is the *co-ordinate ring*

$$K[V] := K[X_1, \dots, X_n]/\mathcal{I}(V)$$

(see, for instance, [15, Chapter II, Proposition 4.4]). As a consequence of the correspondence theorem for prime ideals, it follows that $\dim V \leq \dim K[X_1, \dots, X_n] - 1 - \text{height}(\mathcal{I}(V))$. In fact, since the length of any maximal chain of prime ideals in $K[X_1, \dots, X_n]$ is n (see, for instance, [15, Chapter II Proposition 3.4]), it is not difficult to see that equality holds; that is,

$$(A.2) \quad \dim V = n - 1 - \text{height}(\mathcal{I}(V)).$$

- A projective variety $V \subseteq \mathbb{P}^n(K)$ is a set-theoretic complete intersection if it is the intersection of $n - \dim V$ projective hypersurfaces.

Proof (of Lemma A.1). For $0 \leq r \leq m$ let $I_r := \langle f_1, \dots, f_r \rangle$, where it is understood that $I_0 := \{0\}$. It will be shown, using induction, that $I_0 \subset \dots \subset I_m$ (with strict inclusion) and that each I_r is a prime ideal. Letting $V_0 := \mathbb{P}^{n-1}(\overline{\mathbb{F}}_p)$ and

$$V_r := \{x \in \mathbb{P}^{n-1}(\overline{\mathbb{F}}_p) : f_j(x) = 0 \text{ for } 1 \leq j \leq r\}$$

for $1 \leq r \leq m$, it then immediately follows that the varieties V_r are all irreducible. It is remarked that it is useful to establish the stronger condition that the I_r are prime in order to facilitate the induction.

The case $r = 0$ (corresponding to the trivial ideal $\{0\}$) is vacuous. Fix $1 \leq r \leq m$ and assume, by way of induction hypothesis, that $I_0 \subset \dots \subset I_{r-1}$ and that each I_i is prime for $0 \leq i \leq r-1$.

To show $I_{r-1} \subset I_r$ is a *proper* subset, it suffices to show that $f_r \notin \langle f_1, \dots, f_{r-1} \rangle$. Aiming for a contradiction, suppose that

$$f_r = \sum_{j=1}^{r-1} h_j f_j$$

for some $h_j \in \overline{\mathbb{F}}_p[X_1, \dots, X_n]$. Differentiating the above equation,

$$\frac{\partial f_r}{\partial X_k} = \sum_{j=1}^{r-1} \frac{\partial h_j}{\partial X_k} f_j + h_j \frac{\partial f_j}{\partial X_k}$$

and thus, if $x \in Z(f_1, \dots, f_r)$, then it follows that

$$\frac{\partial f_r}{\partial X_k}(x) = \sum_{j=1}^{r-1} h_j(x) \frac{\partial f_j}{\partial X_k}(x).$$

However, this identity contradicts the non-degeneracy hypothesis (which implies that the vectors $(\frac{\partial f_j}{\partial \vec{X}}(x))_{j=1}^r$ are linearly independent) and so $V_r \subset V_{r-1}$, as claimed.

To prove that I_r is prime it suffices to show:

- i) I_r is radical;
- ii) V_r is irreducible.⁷

The first step towards proving either of these statements is to show that $\text{height}(I_r) = r$. Recall from the induction hypothesis that $\{0\} = I_0 \subset \cdots \subset I_{r-1}$ forms a strictly increasing chain of prime ideals with $I_{r-1} \subset I_r$, which implies that $\text{height}(I_r) \geq r$. Therefore, combining this with the generalised Krull principal ideal theorem, $\text{height}(I_r) = r$, as required.

One may now show that I_r is a radical ideal via a criterion of Serre (see, for instance, [9, Chapter 18]). Let \mathcal{J}_r be the ideal generated by the $r \times r$ minors of the Jacobian matrix

$$\frac{\partial \vec{f}}{\partial \vec{X}} = \frac{\partial(f_1, \dots, f_r)}{\partial(X_1, \dots, X_n)}$$

taken modulo I_r ; that is, \mathcal{J}_r is the ideal of the ring $K[X_1, \dots, X_n]/I_r$ generated by the minors of $\partial \vec{f}/\partial \vec{X}$ viewed as elements of $K[X_1, \dots, X_n]/I_r$. Combining [9, Proposition 18.13] and [9, Proposition 18.15 a)], to show I_r is radical it suffices to show that $\text{height}(\mathcal{J}_r) \geq 1$. This is equivalent to showing $\text{height}(I_r + J_r)/I_r \geq 1$ where J_r is the ideal of $K[X_1, \dots, X_n]$ generated by the minors of $\partial \vec{f}/\partial \vec{X}$. The non-degeneracy condition implies that

$$\mathcal{V}(I_r) \cap \mathcal{V}(J_r) = \{x \in \mathbb{P}^{n-1}(\overline{\mathbb{F}}_p) : f(x) = 0 \text{ for all } f \in I_r + J_r\} = \emptyset$$

and thus, by the Nullstellensatz, $\sqrt{I_r + J_r} = \langle X_1, \dots, X_n \rangle$ and hence $\text{height}(I_r + J_r) = n$. Since $\langle X_1, \dots, X_n \rangle$ is a maximal ideal of $K[X_1, \dots, X_n]$, it follows from the discussion preceding (A.2) that any maximal chain of prime ideals containing $I_r + J_r$ has length n . From this, it follows that

$$\text{height}(I_r + J_r)/I_r = n - r \geq 2,$$

and so I_r is radical.

It remains to demonstrate the irreducibility of $V := V_r$; for this it suffices to show the following two conditions hold:

- i) V is (Zariski) connected;
- ii) V is smooth as a projective variety.

Indeed, any regular point of V lies in precisely 1 irreducible component (see, for instance, [15, Chapter VI, Proposition 1.13]). Thus, if V is smooth, then the irreducible components partition V into disjoint Zariski-closed subsets.

⁷Of course, the irreducibility of V_r is the only property that one is really after here, but the stronger condition that I_r is prime is needed to run the induction argument.

If V is also connected, then V must have a single irreducible component, and so V is irreducible.

By the Nullstellensatz, $\text{height}(\mathcal{I}(V)) = \text{height}(I_r) = r$ and so, recalling (A.2), it follows that $\dim V = n - 1 - r \geq 1$. Since V is, by definition, the intersection of r projective hypersurfaces, V is therefore a set-theoretic complete intersection. The Hartshorne connectedness theorem [15, Chapter VI, Theorem 4.2] now implies that V is connected.

Finally, one may verify that V is smooth using the the Jacobian criterion (see, for instance, [15, Chapter VI, Proposition 1.5]⁸). This states that for every point $x \in V$ one has

$$(A.3) \quad \text{rank} \frac{\partial(f_1, \dots, f_r)}{\partial(X_1, \dots, X_n)}(x) \leq n - 1 - \dim_x V,$$

where $\dim_x V$ is equal to the maximum of the dimensions of the irreducible components of V that contain x and, moreover, if equality holds in (A.3), then V is smooth at x . Note that $n - 1 - \dim V = n - 1 - (n - 1 - r) = r$, which is precisely the rank of the Jacobian matrix, and so one wishes to show that $\dim_x V = \dim V$. To see this, it suffices to prove for any given $x \in V$ that all the irreducible components of V that contain x have the same dimension. Indeed, in this case, since V is connected, it follows that all the irreducible components of V must have the same dimension, and this must then be equal to $\dim V$ (since $\dim V$ is equal to the maximum of the dimensions of the irreducible components by the Nullstellensatz (see [15, Chapter II Proposition 3.11])).

Fixing $x \in V$, consider the prime ideal $\mathfrak{p}_x := \{f \in K[V] : f(x) = 0\}$ (recall $K[V]$ denotes the co-ordinate ring of V). The localisation $K[V]_{\mathfrak{p}_x}$ is Cohen–Macaulay by [9, Proposition 18.8] (see also [15, Chapter VI, Corollary 3.15]) and therefore all the minimal primes of $K[V]_{\mathfrak{p}_x}$ have the same dimension d by [9, Proposition 18.11]. Let W be an irreducible component of V containing x . Thus, by the Nullstellensatz (see [15, Chapter II Proposition 3.11]), W corresponds to a minimal prime ideal $\mathfrak{q} \trianglelefteq K[V]$ with $\mathfrak{q} \subseteq \mathfrak{p}_x$. The localisation $\mathfrak{q}_{\mathfrak{p}_x}$ is a minimal prime of $K[V]_{\mathfrak{p}_x}$ (see [15, Chapter III, Proposition 3.6 and Proposition 4.14]) and $K[V]_{\mathfrak{p}_x}/\mathfrak{q}_{\mathfrak{p}_x} \cong K[V]/\mathfrak{q}$ (see [15, Chapter III, Rule 4.15]). Combining these observations, $\dim W = \dim K[V]/\mathfrak{q} = d$ and so all irreducible components W containing x have the same dimension, as required. \square

The above argument also yields Corollary A.2.

Proof (of Corollary A.2). The proof of Lemma A.1 implies that $\dim V_r = n - 1 - r$ for $1 \leq r \leq \min\{m, n - 2\}$, and it remains only to verify the

⁸The reference [15] only gives the *affine* Jacobian criterion, rather than the *projective* version used here. Both results, however, can be obtained via a similar method of proof.

case $r = m = n - 1$. The first part of the argument used to establish the inductive step shows $\text{height}(I_{n-1}) = n - 1$ and therefore one deduces that $\dim V_{n-1} = 0$, as required. \square

References

- [1] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York-Heidelberg, 1976, Undergraduate Texts in Mathematics. MR 0434929
- [2] Enrico Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430 (1974), 234–241. Lecture Notes in Math., Vol. 383. MR 0429903
- [3] Raf Cluckers, *Igusa and Denef-Sperber conjectures on nondegenerate p -adic exponential sums*, Duke Math. J. **141** (2008), no. 1, 205–216. MR 2372152
- [4] ———, *Exponential sums: questions by Denef, Sperber, and Igusa*, Trans. Amer. Math. Soc. **362** (2010), no. 7, 3745–3756. MR 2601607
- [5] ———, *Analytic van der Corput lemma for p -adic and $\mathbf{F}_q((t))$ oscillatory integrals, singular Fourier transforms, and restriction theorems*, Expo. Math. **29** (2011), no. 4, 371–386. MR 2861764
- [6] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. MR 0340258
- [7] J. Denef and S. Sperber, *Exponential sums mod p^n and Newton polyhedra*, Bull. Belg. Math. Soc. Simon Stevin (2001), no. suppl., 55–63, A tribute to Maurice Boffa. MR 1900398
- [8] Jan Denef, *Report on Igusa's local zeta function*, Astérisque (1991), no. 201-203, Exp. No. 741, 359–386 (1992), Séminaire Bourbaki, Vol. 1990/91. MR 1157848
- [9] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960
- [10] Jonathan Hickman and James Wright, *An abstract L^2 Fourier restriction theorem*, accepted to Math. Res. Let. Preprint: [arXiv:1801.03180](https://arxiv.org/abs/1801.03180).
- [11] ———, *The Fourier restriction and Kakeya problems over rings of integers modulo N* , Discrete Analysis 2018:11 (2018), 54 pp.
- [12] Jun-ichi Igusa, *Forms of higher degree*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 59, Tata Institute of Fundamental Research, Bombay; by the Narosa Publishing House, New Delhi, 1978. MR 546292
- [13] ———, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 2000. MR 1743467 (2001j:11112)
- [14] Neeraj Kumar and Ivan Martino, *Regular sequences of power sums and complete symmetric polynomials*, Matematiche (Catania) **67** (2012), no. 1, 103–117. MR 2927823
- [15] Ernst Kunz, *Introduction to commutative algebra and algebraic geometry*, Modern Birkhäuser Classics, Birkhäuser/Springer, New York, 2013, Translated from the 1980 German original [MR0562105] by Michael Ackerman, With a preface by David Mumford, Reprint of the 1985 edition [MR0789602]. MR 2977456
- [16] Gilles Lachaud and Robert Rolland, *On the number of points of algebraic sets over finite fields*, J. Pure Appl. Algebra **219** (2015), no. 11, 5117–5136. MR 3351576
- [17] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR 0065218
- [18] I. G. Macdonald, *Symmetric functions and Hall polynomials*, second ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1995, With contributions by A. Zelevinsky, Oxford Science Publications. MR 1354144
- [19] S. A. Stepanov, *The number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1171–1181. MR 0252400
- [20] Trevor D. Wooley, *A note on simultaneous congruences*, J. Number Theory **58** (1996), no. 2, 288–297. MR 1393617 (97h:11037)

- [21] James Wright, *Exponential sums and polynomial congruences in two variables: the quasi-homogeneous case*, Preprint: [arXiv:1202.2686](#).

Mathematical Institute, University of St Andrews, North Haugh, St Andrews, Fife, KY16 9SS, UK. (Formerly: Eckhart Hall Room 414, Department of Mathematics, University of Chicago, 5734 S. University Avenue, Chicago, Illinois, 60637, US.)

E-mail : jeh25@st-andrews.ac.uk

URL: <http://www.mcs.st-and.ac.uk/~jeh25/>

Room 4621, James Clerk Maxwell Building, The King's Buildings, Peter Guthrie Tait Road, Edinburgh, EH9 3FD, UK.

E-mail : j.r.wright@ed.ac.uk